شركة هواوي تدخل التاريخ: القوى العظمى ومخاطر الاتصالات السلكية واللاسلكية، 1840-2021

راش دوشي وكيفن ماكغينيس

معهد بروكنجز، مارس 2021

الملخص التنفيذي

في أواخر عام 2018، ووسط المخاوف الأمريكية حول ما إذا كانت كندا سترحب بشركة هواوي في شبكات الاتصالات السلكية واللاسلكية الخاصة بها، أدلى رئيس الوزراء الكندي جاستين ترودو بسلسلة من التصريحات التي استحوذت على الآراء السائدة في أنحاء كثيرة من العالم. فقد صرَّح في ذلك الوقت قائلاً: "يجب ألا يكون قرارًا سياسيًا"، وأضاف أن كندا "لن تسمح للسياسة بالتدخل في القرارات" المتعلقة بدور هواوي الذي تؤديه في شبكتها.[1]

لم تكن فكرة إمكانية فصل سياسات القوى عن التساؤلات حول الاتصالات السلكية واللاسلكية تفاؤلية فحسب، بل كانت أيضًا خارج إطار تاريخ الاتصالات السلكية واللاسلكية. ويستكشف هذا التقرير ذلك التاريخ، ويوضح كيف أن القوة والاتصالات السلكية واللاسلكية كانت في الغالب مرتبطة ارتباطًا وثيقًا. وعندما تجاهلت الدول هذه الروابط ولم تبالِ بأمن شبكاتها، كانت النتائج في غير صالحها بل وكانت مأساوية في بعض الأحيان.

يتناول هذا التقرير عدّة حالات بارزة للتنافس بين القوى العظمى في مجال الاتصالات السلكية واللاسلكية تعود إلى البداية المبكرة للاتصالات السلكية واللاسلكية الكهربائية في أربعينيات القرن التاسع عشر. وتُظهِر هذه الحالات أن العديد من التساؤلات التي يواجهها صناع السياسات اليوم لها نظائر مشابهة جدًا من الماضي. على الرغم من أن المناقشة الدائرة حاليًا حول أمن الشبكات والبنية الأساسية لشبكات الجيل الخامس قد تبدو جديدة، فإنها في واقع الأمر تعكس نزاعات قديمة تعود إلى فجر عصر الاتصالات السلكية واللاسلكية الكهربائيّة بنحو 150 سنة. فضلاً عن ذلك، فإن العديد من عناصر المنافسة المعروفة اليوم في مجال الاتصالات السلكية واللاسلكية، مثل استخدام هيئات وضع المعايير وأشكال الدعم الحكومية وعمليات التنصت على الكابلات وحرب المعلومات وأسواق البلدان النامية والتشفير لكسب الميزة، موجودة قبل أكثر من قرن من الزمان، وتقدِّم دروسًا مهمة يستفاد منها في المناقشات الحالية.

ترد أدناه قائمة بهذه الدروس الرئيسية:

1. **إنَّ السيطرة على شبكات الاتصالات السلكية واللاسلكية العالمية تمثِّل شكلاً من أشكال القوة السياسية.** من المتوقع أن تشكل شبكات الجيل الخامس حجر الأساس لاقتصاد أكثر ذكاءً واتصالاً يربط بين عدد لا يحصى من أجهزة الاستشعار وغيرها. ومن منطلق حرص الصين على بناء هذه الشبكات في مختلف أنحاء العالم، فقد عمِلت على دعم شركاتها ومشروعاتها الرائدة في مجال تقنية الجيل الخامس في مختلف أنحاء العالم كجزء من مبادرة "طريق الحرير الرقمي". ويشابه هذا الجهد سعيَ بريطانيا العظمى إلى فرض هيمنتها على الشبكة مع بزوغ فجر اختراع التلغراف الكهربائي. فقد نجحت بريطانيا في بناء ميزتها على مدى ستة عقود من الزمان من خلال زيادة اعتماد دول أخرى بشكل مطّرد على شبكاتها ــ لدرجة أنها تغاضت عن الرسوم والفوائد الاقتصادية لإغراء هذه الدول لتمرير الكابلات عبر بريطانيا ــ في حين أنها نجحت أيضًا في الحد من اعتمادها على الشبكات الأجنبية. وفي نهاية المطاف، سيطرت على أكثر من نصف حركة الاتصالات الكابلية على مستوى العالم، وأكبر شبكة لاسلكية، وأكبر أسطول من سفن مد الكابلات. فإن "الهيمنة المعلوماتية" لبريطانيا قد مكَّنتها من عزل ألمانيا عن كل الاتصالات السلكية واللاسلكية العالمية تقريبًا في الحرب العالمية الأولى، فضلاً عن أنها أرغمت برلين على توجيه حركة الاتصالات عبر الخطوط المملوكة لبريطانيا التي تخضع للمراقبة البريطانية، وقد ثبت في ما بعد أن هذه الخطوة كانت حاسمة في هزيمة ألمانيا في الصراع.

2. **إنَّ فترات السلام والازدهار طويلة الأجل تؤدي عمومًا إلى حالة من اللامبالاة تجاه مخاطر الاتصالات السلكية واللاسلكية.** في السنوات الثلاثين الماضية، تزامن السلام والعولمة الاقتصادية في مرحلة ما بعد الحرب الباردة مع التقدم السريع في مجال الاتصالات السلكية واللاسلكية الذي دفع الدول إلى إعطاء الأولوية للفوائد التجارية الثورية على المخاطر السياسية والأمنية، بما في ذلك أيضًا الملكية الأجنبية للشبكات أو تشغيلها الأجنبي. حدث تطور مماثل مع بزوغ فجر الاتصالات السلكية واللاسلكية في أربعينيات القرن التاسع عشر، وهو ما تزامن أيضًا مع فترة من السلام النسبي والعولمة استمرت حتى الحرب العالمية الأولى. وفي فترة كبيرة من تلك الحقبة، كانت الرغبة في الاستفادة من الإمكانات التجارية التي بدت خارقة لتقنيات الاتصالات الجديدة سببًا في حجب التساؤلات حول الاعتماد على الشبكات أو الشركات الأجنبية. فقد استفادت بريطانيا العظمى من استسلام الدول الأخرى لحالة اللامبالاة من خلال بناء مكانة عقدية حصينة في الشبكات العالمية ثم استغلال هذه المكانة، مع اعتماد أغلب القوى العظمى الأخرى على شبكاتها.

3. **عندما تكون الدول في حالة من اللامبالاة تجاه أمن اتصالاتها السلكية واللاسلكية، فإن النتائج قد تكون مأساوية وقد تعيد تشكيل السياسة العالمية.** إنَّ العقود التي عاشتها ألمانيا في حالة من اللامبالاة تجاه اعتمادها على خطوط الاتصالات السلكية واللاسلكية البريطانية كانت تعني أنه بحلول الوقت الذي انتبهت فيه برلين إلى مخاطر هذا الاعتماد، كان قد فات الوقت لتغيير هذا الاعتماد. فعندما اندلعت الحرب العالمية الأولى، قطعت بريطانيا كل الكابلات الألمانية وأرغمت برلين على توجيه حركة الاتصالات عبر الشبكات البريطانية على الرغم من خطر اعتراضها، الأمر الذي أدى إلى اكتشاف "برقية زيمرمان" وفك شفرتها، التي ساعدت على حمل الولايات المتحدة على الدخول في الحرب. وعلى نحو مماثل، سمح عدم الانضباط الروسي في عمليات الإرسال اللاسلكي في الحرب العالمية الأولى للألمان باعتراض المراسلات، و"رؤية" حركة القوات الروسية في الوقت الحقيقي، والتعامل معها بوصفها هزيمة حاسمة في معركة تاننبرغ. ثم في الحرب العالمية الثانية، أدت ثقة ألمانيا النازية المفرطة بشفراتها إلى فك هذه الشفرات بأقل مجهود ممكن، الأمر الذي سمح لبريطانيا العظمى بتفسير الرموز والحصول على المعلومات الاستخباراتية التي يُعتَقَد أنها اختصرت فترة الحرب بما يتراوح بين عامين وأربعة أعوام. فبسبب قوة المعلومات، قد تؤدي حالات عدم الانضباط أو اللامبالاة تجاه إشارات المعلومات، حتى وإن كانت من حين إلى آخر، إلى تغير التاريخ.

4. **إنَّ التقنية الجديدة تؤدي دومًا إلى بذل جهود جديدة لاعتراضها.** لقد أدى ظهور الكابلات الممتدة تحت سطح البحر إلى بذل جهود لقطع هذه الخطوط والتنصت عليها في وقت مبكر من الحرب الإسبانية الأمريكية؛ وأدى الإرسال اللاسلكي إلى بذل جهود من قِبَل المتنافسين للوصول إلى عُقد الشبكة واعتراض عمليات الإرسال؛ كما أدى ظهور أنظمة تشفير متطورة إلى بذل جهود صناعية لاختراق هذه الأنظمة. وفي كل حقبة، كان بعض الناس يعتقد أن قفزة جديدة في الاتصالات السلكية واللاسلكية قد تكون أقل عُرضة للخطر من تلك التي سبقتها. بيد أن دورة الإبداع والاستغلال استمرت في كل مرة.

5. **لم تكن شبكات الاتصالات السلكية واللاسلكية محايدة سياسيًا على الإطلاق، خصوصًا في أوقات التوتر.** في عام 2019، تعهد المسؤولون التنفيذيون في هواوي بعدم التجسس أو التسلل، وقطعوا وعدًا بأن شركتهم ستظل بعيدة عن السياسة، مع التزام الحكومة الصينية باحترام هذا التعهد. لكن قبل أكثر من قرن من الزمان، قدَّمت شركات الاتصالات السلكية واللاسلكية والحكومات المضيفة لها وعودًا مماثلة علنًا، في حين نَقَضتْ هذه الوعودَ سرًا وتعمل الآن معًا في وقتَي السلم والحرب. على سبيل المثال، دفعت الهيمنة البريطانية على الكابلات البحرية الفرنسيين والألمان والأمريكيين إلى المطالبة بإبقاء هذه الخطوط محايدة، حتى في حالة الحرب. وصرحت الشركات البريطانية بحياديتها علنًا، لكنها في واقع الأمر أذعنت للمصالح السياسية البريطانية، خصوصًا في لحظات التوتر الشديد، وتخلت عن هذه الحيادية تمامًا خلال فترات الحرب. وكانت القوة التي تأتي من تعطيل تدفقات المعلومات المنافسة أو اعتراضها مغرية عمومًا لدرجة يصعب معها صمود المزاعم الصادقة بالحيادية.

6. **كثيرًا ما تسعى الدول إلى بناء شركاتها الخاصة الرائدة في الاتصالات السلكية واللاسلكية بمجرد إدراكها الضعف الناتج عن الاعتماد على الشركات المنافسة أو الشركات المعادية.** تفتقر الولايات المتحدة حاليًا إلى شركة تصنيع رئيسية لمحطات قاعدية لشبكات الجيل الخامس، ما أثار مناقشات حول ما إذا كان ينبغي لها أن تستثمر في شركاتها الخاصة أو تعتمد على شركات حليفة. كما أثار ذلك الخلافَ حول الدرجة التي تحتلها شركة هواوي نفسُها كعملاق

دولة بحكم الأمر الواقع. والواقع أن هذه المناقشات ليست بجديدة. ففي أوائل القرن العشرين، بدأت العديد من الدول التي تعتمد على دول أخرى في تصنيع معدات أو شبكات الاتصالات السلكية واللاسلكية ببناء أنظمة خاصة بها. على سبيل المثال، دفعت ألمانيا شركتين ألمانيتين إلى العمل مع شركات منافسة في مجال اللاسلكي، مثل "سيمنز وهالسكي" و"إيه إي جي"، لإنشاء بديل ألماني للهيمنة البريطانية في مجال الإرسال اللاسلكي. كما دعمت العديد من الدول الرائدة الأخرى الشركات التي كانت متشابكة مع الدول التي دعمت هذه الشركات، على الرغم من كونها شركات خاصة ظاهريًا.

7. **من الممكن أن يحدد الصراع من أجل معايير الاتصالات أيّ الدول ستمارس قوة الشبكة، وهو يتطلب غالبًا تجنيد الحلفاء والشركاء.** تستطيع الدول التي تصبح التكنولوجيا فيها المعيارَ المهيمن أن تمارس نفوذها على الآخرين. وعلى هذا النحو، فإن المنافسة الحالية على معايير تكنولوجيا المعلومات والاتصالات أشبه بالمنافسة بين الإنجليز والألمان على الشبكات اللاسلكية. كانت بريطانيا مهيمنة جدًا، من خلال شركة ماركوني التي تدعمها، على أجهزة الراديو اللاسلكية إلى الحد الذي اضطر كافة القوى العظمى الأخرى إلى تمرير رسائل عبر الشبكة اللاسلكية البريطانية، التي رفضت التعامل مع أي محطات لاسلكية أخرى. وفي نهاية المطاف، وجدت ألمانيا النجاح في كسر هذه الهيمنة في هيئة تضع المعايير وتحظر سياسة "عدم الاتصال المتبادل" هذه بمساعدة قوى أخرى، منها الولايات المتحدة وفرنسا ـ وهذا دليل على مدى إمكانية استخدام دول ليبرالية لنُهج ائتلافية مماثلة اليوم من أجل وضع معايير مواتية لتكنولوجيا المعلومات والاتصالات أو الحفاظ عليها إذا ما نجحت في العمل معًا.

8. **تتجه الدول إلى التشفير كلما أصبحت إمكانية اعتراض اتصالاتها أسهل، لكن غالبًا ما تكون لهذا التشفير حدود بسبب الخصوم المصمِّمين أو أخطاء المستخدمين.** يزعم بعض الناس أن المخاوف بشأن الدور الذي تؤديه شركة هواوي في الشبكات أو بشأن تعرض الأجهزة المتصلة بالإنترنت للخطر بشكل عام تقل بسبب طرق التشفير الحديثة. وهذه الأنواع من المزاعم لها تاريخ طويل. فمع بزوغ فجر الاتصالات السلكية واللاسلكية قبل قرن من الزمان، كان احتمال قراءة رسائل التلغراف من قِبَل آخرين كانوا يسيطرون على عُقَد الشبكة، أو احتمال أن يتم اعتراض الإرسال باستخدام أجهزة تنصت غير مرصودة، سببًا في حدوث تطورات كبيرة في التشفير تولد عنها فرط الثقة من حين إلى آخر. وكان يُعتقد أن آلات التشفير الدوارة المعقدة في ألمانيا غير قابلة للاختراق، لكن أخطاء المستخدمين لهذه الآلات والجهود الصناعية البريطانية سمحت لبريطانيا العظمى بفك الشفرة الألمانية. وكان من الممكن أن تؤدي التحديثات منخفضة التكاليف للمعدات وأنظمة التشفير الألمانية إلى التغلب على الميزة التي تمتعت بها بريطانيا، لكن فرط ثقة برلين في آليات تشفيرها كان سببًا في الحيلولة دون هذه التعديلات، الأمر الذي أسفر عن اعتراض معلومات استخباراتية أعادت تشكيل مسار الحرب. إنَّ التشفير التام أكثر تقدمًا مقارنة بجهود التشفير السابقة، لكن يشير التاريخ إلى ضرورة التواضع بعض الشيء.

9. **تستهين دول كثيرة بالدرجة التي قد يبذل بها الخصم جهودًا غير عادية لاختراق شبكاتها.** وسط المناقشات الدائرة حول الاتصالات السلكية واللاسلكية الحديثة، تجدر الإشارة إلى أن الدول التي أعطت الأولوية إلى وسائل الراحة أو التجارة، التي اتخذت تدابير أمنية ضعيفة نتيجة لذلك، قد صُدِمت في الغالب بالجهود التي يبذلها خصم مصمِّم لاختراق شبكاتها أو الإضرار بها. في الحرب العالمية الأولى، فوجئت ألمانيا بسرعة بريطانيا وقسوتها عندما قطعت كل الكابلات التي كانت تستخدمها ألمانيا للتواصل مع العالم الخارجي؛ وعلى نحو مماثل، فوجئ القادة الروس عندما أدى عدم الانضباط في عمليات الإرسال اللاسلكي إلى هزيمة كارثية في تاننبرغ. وفي الحرب العالمية الثانية، لم تكن ألمانيا تتوقع من البريطانيين أن يؤسسوا عملية فك تشفير صناعية شديدة المركزية وقادرة على استغلال أخطاء الاتصالات الألمانية ـ مهما كانت بسيطة أو عابرة ـ لفك الشفرة الألمانية. وفي أثناء الحرب الباردة، لم يشفر السوفييت على الإطلاق خطَّ الهاتف الداخلي الممتد تحت سطح الماء واعتقدوا بأن الولايات المتحدة لن تصل إليه، لكن واشنطن وجدت وسيلة للتنصت عليه ـ ما أكسبها مصدرًا للمعلومات الاستخباراتية لا يقدر بثمن.

10. **لا يتعلق أمان الشبكة بالاعتراض فحسب، بل بالحرمان منها أيضًا.** إنَّ بعض المناقشات الدائرة حول دور هواوي في الشبكات تركِّز على تساؤلات حول أمن البيانات، لكن قد تكون هناك استفادة من إمعان النظر في الحرمان من الشبكات، الذي كان ولا يزال يشكل جزءًا مهمًا من المنافسة بين القوى العظمى في مجال الاتصالات. فقد شهدت المرحلة المبكرة من اختراع التلغراف سعيَ القوى العظمى إلى قطع الكابلات والحرمان من الاتصالات، الأمر الذي بلغ ذروته بعملية بريطانيا العظمى غير المسبوقة التي خُطِّط لها جيدًا لقطع كل الكابلات في مختلف أنحاء العالم التي قد تصل ألمانيا بالعالم الخارجي. ففي بعض الأحيان، قد تضر الدولة بنفسها عند اتباع إستراتيجيات الحرمان من الشبكات، لكنها رغم ذلك ستستمر إذا كانت تعتقد أن الضرر الواقع عليها أعظم من الضرر الذي قد يلحق بخصمها.

القوى العظمى والاتصالات السلكية واللاسلكية

يقول أحد مؤرخي الاتصالات السلكية واللاسلكية "إن الإمبراطوريات الكبرى بذلت جهودًا هائلة لتسريع تدفق المعلومات. فقَدْ شيَّد الرومان الطرق، وأقام الفرس والمغول محطات لإبدال الخيول، ودَعَم البريطانيون بواخر البريد".[2] لكن على الرغم من سعي الدول الحثيث إلى الحصول على المعلومات، فإن تدفقات هذه المعلومات ظلت محدودة حتى بزوغ فجر التلغراف الحديث. فقد أدت كهربة تدفقات المعلومات إلى ظهور الاتصالات الحديثة، وصاحبتها أنماط مألوفة من منافسة القوى العظمى عليها.

إنَّ العقود الأولى من الاتصالات الحديثة، التي امتدت من عام 1840 إلى الحرب العالمية الأولى، تشترك في سمات مهمة مع الوقت الحاضر. كانت تلك الفترة، مثلها في ذلك كمثل عصر ما بعد الحرب الباردة، واحدة من فترات السلام النسبي بين القوى العظمى الذي جعل الدول الرائدة "أقل حساسية" تجاه المسائل السياسة والأمنية المتعلقة بشبكات الاتصالات السلكية واللاسلكية.[3] ومع بناء القوى العظمى للشبكات الوطنية والدولية في القرن التاسع عشر، كان الكثير مقتنعًا بإسناد مسؤولية ذلك إلى الصناعة، وتجاهُل جنسية الشركات الخاصة، والتقليل من مخاطر سيطرة الخصم على شبكات الاتصالات السلكية واللاسلكية. وكانت الفوائد المترتبة على التغيرات الثورية في الاتصالات السلكية واللاسلكية ـ التي أطلق عليها البعض في ذلك الوقت "إبادة الزمان والمكان"[4] ـ واضحة ومربكة إلى الحد الذي جعل "ملكية الكابلات تشكل قضية ثانوية".[5] كان الهدف من اختراع التلغراف هو الأعمال أكثر من كونه هدفًا سياسيًا في تلك الفترة، كما يشير أحد المؤرخين في ملاحظة قد تنطبق بمنتهى البساطة على بعض الجدل الأولي الذي أثير حول تكنولوجيا المعلومات الحديثة وأحدث ما وصلت إليه: الجيل الخامس.[6]

لم تكن لتدوم هذه الفترة من اللامبالاة النسبية بين القوى العظمى. فقد كانت هناك دول مثل بيرو في عام 1879 ثم الولايات المتحدة في عام 1898 من أوائل الدول التي قطعت شبكات الاتصالات لمنافسيها. ومع تصاعد التوترات بين القوى العظمى، أفاقت دول في مختلف أنحاء العالم لكي تجد أن بعض الدول ـ بريطانيا العظمى على وجه التحديد ـ قد نجحت في تحقيق السلام طويل الأجل، ومن خلال شركاتها الخاصة، فرضت نفوذًا قويًا على الاتصالات الدولية.

بسبب الخوف المتزايد من الاعتماد على شبكات الكابلات البريطانية الممتدة تحت سطح البحر، قدَّمت دول مثل فرنسا وألمانيا إعانات دعم كبيرة لتطوير شبكاتها الخاصة بما لا يختلف كثيرًا عن الدعم والحماية اللذين تقدِّمهما الصين إلى شركاتها الكبرى في مجال تكنولوجيا المعلومات مثل علي بابا، وبايدو، وتينسنت، وهواوي. وكما وثَّقت المؤرخة هايدي توريك في كتابها، فإن الدول المنافسة لبريطانيا راهنت بشكل كبير أيضًا على الجيل التالي من تقنية الاتصالات ــ "الإرسال التلغرافي اللاسلكي"، المشهور بالراديو ــ على أمل الحد من الاعتماد على كابلات التلغراف البريطانية الممتدة تحت سطح البحر.[7] وعلى الرغم من ريادة بريطانيا في هذا المجال، فقد رفضت ألمانيا الاعتماد على الشبكات البريطانية. فقد بنت شبكتها الخاصة مع شركات رائدة مدعومة من قِبل الدولة وتعمل جاهدة على تثبيت أقدامها في أجزاء أقل اتصالاً من العالم ـ أمريكا اللاتينية، وإفريقيا، وآسيا ـ وهذا ما قد يعكس اليوم توسع نشاط شركات التكنولوجيا الصينية في العالم النامي وتصميم بكين على إرساء الأسس اللازمة لشبكات الجيل الخامس.

طوال هذه الفترة، كانت دول هذا العصر تتعامل بجدية تامة مع كثير من عناصر المنافسة بين القوى العظمى في مجال الاتصالات السلكية واللاسلكية، خلافًا لما هو عليه الحال اليوم من عدم الانتباه أحيانًا إلى هذه العناصر. فبعد الإحباط الذي أصاب ألمانيا من الهيمنة البريطانية على الشبكات اللاسلكية، لجأت إلى هيئة لوضع المعايير لكسر الهيمنة البريطانية ــ وهو التكتيك الذي أظهر أن هذه الهيئات لم تكن أقل أهمية في ذلك العصر من حالها الآن. ومع تحول الاتصالات إلى شكلها اللاسلكي وسهولة اعتراضها أكثر من ذي قبل، وضعت القوى العظمى ثقتها في التشفير ــ متجاهلة في بعض الأحيان التشغيل المنضبط لشبكاتها على افتراض أن "أنظمة التشفير" ــ تلك الخطوات المعقدة لتشفير الرسائل أو فك تشفيرها ــ ستحل المشكلة، وهو اعتقاد ثبت أنه كان خاطئًا في كل الأحوال تقريبًا بسبب خطأ المستخدم الوارد حدوثه. والواقع أن لهذا الرأي أوجه تشابه بارزة مع الافتراضات الحديثة حول انعدام الأمان العام لشبكات الاتصالات، والاعتقاد الذي عبر عنه البعض في المناقشات الدائرة حول شركة هواوي بأن التشفير من شأنه أن يعمل إلى حد كبير على تحييد خطورة قدرة الصين على الوصول إلى شبكة الاتصالات.

عندما انتهت فترة السلام بين القوى العظمى واندلعت الحرب، باتت الأهمية السياسية للاتصالات ــ التي لم تكن واضحة دومًا في زمن السلم ــ واضحة فجأة. وكان النجاح الألماني في اعتراض عمليات الإرسال الروسية في الحرب العالمية الأولى سببًا في تحقيق نصر شامل في معركة تاننبرغ لدرجة أنه غير مسار الحرب وساعد على التعجيل بخروج روسيا من الصراع.

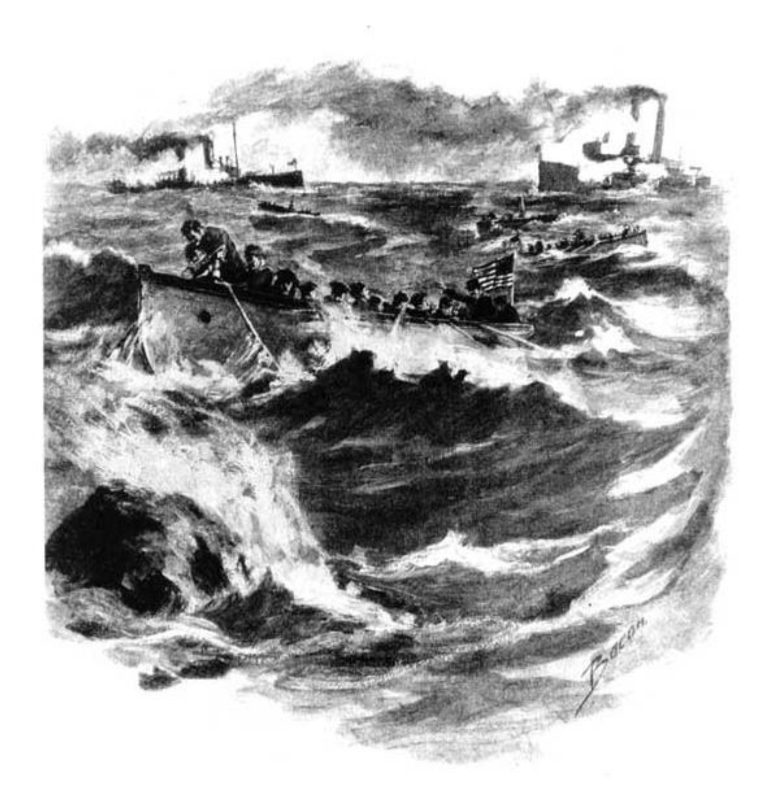
كانت الهيمنة البريطانية على الكابلات الممتدة تحت سطح البحر في الحرب العالمية الأولى هيمنة كاملة إلى الحد الذي أدى إلى عزل ألمانيا عن نظام الاتصالات العالمي، وتمرير حركة الاتصالات الكابلية الألمانية عبر شبكات بريطانيا الخاصة، واكتشاف برقية زيمرمان في نهاية المطاف وفك شفرتها، التي ساعدت على حمل الولايات المتحدة على الدخول في الصراع. وفي الحرب العالمية الثانية، حققت بريطانيا نجاحًا استخباراتيًا آخر من خلال فك التشفير الألماني الذي كان من المفترض أنه غير قابل للاختراق، الأمر الذي أدى إلى الحصول على معلومات استخباراتية لا نظير لها يزعم التاريخ الرسمي البريطاني أنها نجحت في تقصير مدة الحرب في أوروبا بسنوات. وتبرهن هذه الحالات على أن أمن الاتصالات ليس مجرد مسألة تكتيكات خاصة بساحة المعركة، بل هو مسألة منافسة سياسية، وهو أمر يمكن أن يحدد مصائر القوى العظمى وشكل تاريخ العالم.

مع دخول العالم في حرب باردة بين الولايات المتحدة والاتحاد السوفييتي، لم تكن القوة الأمريكية وحدها هي التي تزاحم المزايا البريطانية، بل كانت تزاحمها أيضًا التحولات التكنولوجية التي جعلت الشبكات القديمة أقل أهمية، الأمر الذي أظهر أهمية بقاء القوى العظمى في طليعة الدول المتسلحة بالتكنولوجيا. وفي هذا العصر الجديد، استمرت المنافسة في مجال الاتصالات على أسس مألوفة. على سبيل المثال، أصبحت الولايات المتحدة رائدة في ابتكار طرق جديدة للتنصت على الكابلات البحرية التي دُفِنت في أعماق كبيرة وعُدَّت آمنة لدرجة أن الرسائل التي كانت ترسل عبرها كانت غير مشفّرة في كثير من الأحيان. كما انتقلت المنافسة إلى مجالات أخرى، مثل الأقمار الصناعية والبنية الأساسية للإنترنت، على الرغم من أن كثيرًا من تاريخ هذه المنافسة لا يزال يُكتب، وفي معظم الحالات، يظل سريًا.

كما تبين هذه السلسلة القصيرة من الحالات، كانت الاتصالات ولا تزال سياسية. بشكل عام، كان تطور هذه التقنيات والقدرات مصحوبًا بتطور آخر في طرق استغلال هذه التقنيات والقدرات. فبمجرد ظهور أساليب الاتصال الجديدة، كانت القوى العظمى تبحث عمومًا عن سبل لاعتراضها أو إيقافها. "يقول أحد مؤرخي الاتصالات السلكية واللاسلكية: "إن الاتصالات الكهربائية كثيرًا ما كانت توصف بأنها واحدة من أعظم إنجازات البشرية، لكن عندما ننظر إليها من وجهة نظر أمنية، فإننا نرى صورة مختلفة تمامًا، لأن الأمن ليس خاصية فنية، بل خاصية اجتماعية وسياسية". ويضيف قائلاً: "ما دامت السياسة لم تتحسن، فإن الاتصالات تشكل جانبًا مظلمًا".[8]

ننتقل الآن إلى موجز للموضوعات الرئيسية في ما يقرب من قرنين من المنافسة في مجال الاتصالات.

1. الحرب الإسبانية الأمريكية: حدود حيادية الكابلات



صورة للحملة العسكرية الأمريكية لقطع الكابلات في سينفويغوس نشرت في عام 1907. قد أثبتت العملية أن كابلات التلغراف الممتدة تحت سطح البحر لن تُعامل على أنها حيادية في أثناء الصراع المسلح، حتى من قِبل قوة عظمى كانت تطالب ذات يوم بحيادية الكابلات.

المصدر: *Naval Historical Center Online Library*[9]

مع بدء الكابلات البحرية في التشابك عبر العالم في القرن التاسع عشر، دعت العديد من القوى الرائدة ــ بما في ذلك فرنسا وألمانيا والولايات المتحدة ــ إلى إبقائها معزولة عن السياسة الدولية. ففي عام 1858، وفي واحدة من أولى البرقيات العابرة للمحيط الأطلسي على الإطلاق، حث الرئيس الأمريكي جيمس بيوكانان الملكة فيكتوريا على ضمان الحفاظ على خطوط التلغراف الجديدة على مستوى العالم "حيادية إلى الأبد... حتى في خضم الأعمال العدائية".[10]

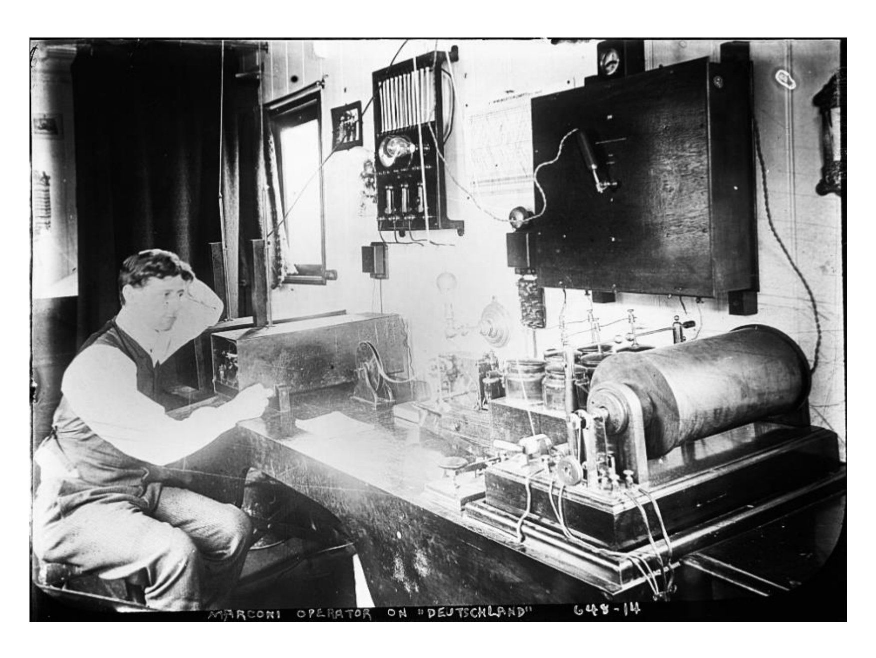
لكن بمجرد اندلاع الأعمال العدائية، هُجِرت مبادئ الحيادية السامية. فبعد مرور عقدين من الزمان على رسالة بيوكانان، قطعت بيرو خطوط الكابلات التشيلية التي كانت تمتد إلى مناطق متنازع عليها.[11] ولم يلق هذا النزاع قدرًا كبيرًا من الاهتمام، لكن عندما قامت الولايات المتحدة ـ التي كانت نصيرًا سابقًا لمبدأ حيادية الكابلات ـ بقطع الكابلات في كل من المحيطين الأطلسي والهادئ خلال الحرب الإسبانية الأمريكية، انتبه العالم إلى ذلك.

كان قد تم التخطيط للعملية الأمريكية لقطع الكابلات قبل اندلاع الصراع. وفي مسرح المحيط الأطلسي، كانت الولايات المتحدة تأمل في فصل إسبانيا عن قواتها في كوبا. ذكرت إحدى المجلات الأمريكية في ذلك الوقت أن "عزل هافانا كان بطبيعة الحال بالغ الأهمية، الأمر الذي تطلب من الولايات المتحدة منع هافانا من أي اتصال برقي مع العالم الخارجي".[12] بدأت الولايات المتحدة بقطع حركة الاتصالات الإسبانية التي كانت تمر عبر الأراضي الأمريكية في فلوريدا. ثم أرسلت مجموعة صغيرة من الجنود الأمريكيين لتدمير عقدة اتصالات رئيسية في سينفويغوس، فعزلت مدينة هافانا وجزءًا كبيرًا من غرب كوبا عن إسبانيا. وبعد ذلك، هاجمت الولايات المتحدة كابلات مختلفة في شرق كوبا، وكذلك كابلات في البحري الكاريبي كانت تربط بورتوريكو بإسبانيا. [13]فأدّى قطع الكابلات إلى إضعاف قدرة إسبانيا على توجيه قواتها في كوبا وقيادتها إلى حد كبير.[14]

في المحيط الهادئ، قطعت الولايات المتحدة الكابل البحري الوحيد بين مانيلا وهونغ كونغ، فعزلت الفلبين فعليًا عن إسبانيا.[15] وقد أضر القرار بالاتصالات الأمريكيّة أيضًا، لكن كان من المفترض أنه ينطوي على ضرر أكبر للإسبان، وقد تمكنت الولايات المتّحدة من تعويض هذا الضرر بإرسال سفينة واحدة بشكل منتظم إلى هونغ كونغ لإرسال الرسائل إلى واشنطن.[16] كما قطعت القوات الأمريكية كابلات بحرية داخل الفلبين، الأمر الذي زاد من إضعاف قدرة إسبانيا على قيادة قواتها.

لعل الحرب الإسبانية الأمريكية كانت الصراع العالمي الأول الذي امتد إلى العديد من المسارح التي تشكل الاتصالات الكهربائية فيها أهمية كبرى. وكانت هذه هي المرة الأولى التي تسعى فيها قوة عظمى إلى حرمان أخرى من الوصول إلى الكابلات البحرية. قبل اندلاع الصراع، كان اختراع التلغراف لا يزال يُنْظَر إليه على أنه مجال تجاري في المقام الأول، وكان هناك كثيرون يتمنون أن تظل الكابلات بعيدة عن المنافسة السياسية والعسكرية. ولقد أثبت الصراع مدى قصور وجهات النظر هذه، وأوضح أن السيطرة على البنية الأساسية للاتصالات والقدرة على حرمان المنافسين الجيوسياسيين من هذه المزايا كانت دومًا ذات أهمية سياسية بالغة.

2. المنافسة الأنجلو ألمانية: بناء الشبكات ووضع المعايير



عامل لاسلكي في شركة ماركوني في "غرفة ماركوني" التابعة لعابرة المحيط الألمانية إس إس دويتشلاند. كان تأثير شركة ماركوني عظيمًا لدرجة أنه تم تشغيل موظفيها في غرف اللاسلكي الألمانية على الرغم من أن ألمانيا كانت قلقة بشأن مخاطر الاعتراض والحرمان.

المصدر: Library of Congress, George Grantham Bain Collection[17]

إنَّ وضع المعايير التكنولوجية، وما يصاحبها من تأثيرات الشبكات، يشكل ساحة قديمة ودقيقة للمنافسة بين القوى العظمى. تستطيع الدول التي تصبح التكنولوجيا فيها المعيارَ المهيمن أن تمارس نفوذها على الآخرين - وهي نقطة لم تغب عن القوى الصاعدة، التي كثيرًا ما تعمل على الحد من مدى تأثرها بذلك من خلال إنشاء أنظمة موازية. والواقع أن المنافسة الصينية الأمريكية الحالية على تكنولوجيا المعلومات والاتصالات تعكس سباقًا منذ قرن من الزمان بين ألمانيا وبريطانيا العظمى لفرض الهيمنة على البنية الأساسية لتكنولوجيا المعلومات والاتصالات في ذلك العصر، مع أوجه تشابه غير عادية ودروس رئيسية يُستفاد منها في الوقت الحاضر.

في أواخر القرن التاسع عشر، قام المهندس الإيطالي غوليلمو ماركوني، بدعم من البحرية الملكية البريطانية، باختراع تقنية الإرسال التلغرافي اللاسلكي.[18] كان هذا الاختراع ثوريًا. وعلى الرغم من أن القوى العظمى كانت تقطع كابلات بعضها بعضًا في الماضي، وكانت الاتصالات بين السفن وبعضها وبين السفن والشاطئ صعبة في ما سبق، فإن نظام ماركوني حل هذه المشكلات وكان أقل عُرضة للتداخل.[19] وفي نهاية المطاف، دخل ماركوني في شراكة مع بريطانيا العظمى ليمنحها احتكارًا للإرسال اللاسلكي. وعند الجمع بين ذلك وبين حصة بريطانيا التي بلغت 60% من شبكة الكابلات الممتدة تحت سطح البحر على مستوى العالم، هيمنت بريطانيا على عمليات الإرسال الدولية. كانت الميزة البريطانية مقلقة بالنسبة إلى ألمانيا، لكن المنافسة على التقنيات اللاسلكية "أتاحت الفرصة أيضًا لألمانيا لتمارس سيطرتها على بنية أساسية دولية جديدة" و"التحايل على الكابلات البريطانية"؛ وارتبطت أسبقية القوة العظمى بالنتيجة.[20]

مع شعوره بالضعف، صرح القيصر فيلهلم الثاني بتقديم الدعم المباشر من الدولة إلى العلماء والمهندسين الألمان بعد أن نجحوا في نسخ تصميمات ماركوني، وتسجيلها ببراءات اختراع داخل ألمانيا، وبناء شبكاتهم اللاسلكية الخاصة التي مُوِّلت بموجب عقود مع المؤسسة العسكرية الألمانية.[21] وعلى الرغم من ذلك، فإن ميزة ماركوني الفائقة المتمثلة في الأسبقية والإرسال اللاسلكي الأبعد مدى كانت سببًا في ترسيخ شركته المدعومة من بريطانيا بوصفها المعيار العالمي، واستفاد ماركوني من هذه التأثيرات الشبكية في اتباع سياسة "عدم الاتصال المتبادل" مع مشغلي اللاسلكي غير الماركونيّ. ولم تكن الشركات وعابرات المحيط الألمانية مستعدة لعزلها عن الاتصال العالمي، لذا فقد فضلت النظام الذي تدعمه بريطانيا على النظام الألماني.

عمل القيصر فيلهلم الثاني على تكثيف السياسة الصناعية الألمانية لمنافسة هذا المعيار البريطاني. فقد أصدر مرسومًا عاجلاً بأن تتحد شركتان ألمانيتان كبريان في مجال الكهرباء وقادرتان على المنافسة في مجال الإرسال اللاسلكي، وهما "سيمنز وهالسكي" و"إيه إي جي"، للعمل معًا لتأسيس شركة تيليفونكن الألمانية كبديل نهائي. ولقد أوضح القيصر أن: "المنافسة [المحلية] في مجال الإرسال التلغرافي اللاسلكي تضعف من القدرة التنافسية لألمانيا، وتمنح شركة ماركوني الفرصة للوصول إلى احتكار عالمي، ولم يكن ذلك في مصلحة ألمانيا".[22] في عهد قيصر فيلهلم الثاني، تبنت ألمانيا تدابير الحماية بحظر أنظمة ماركوني في بعض الحالات. وقد استهدفت الأسواقَ الناشئة عن طريق بيع تقنيتها إلى أمريكا الجنوبية وإفريقيا لوضع المعايير في هذه المناطق وتأمين العائدات.

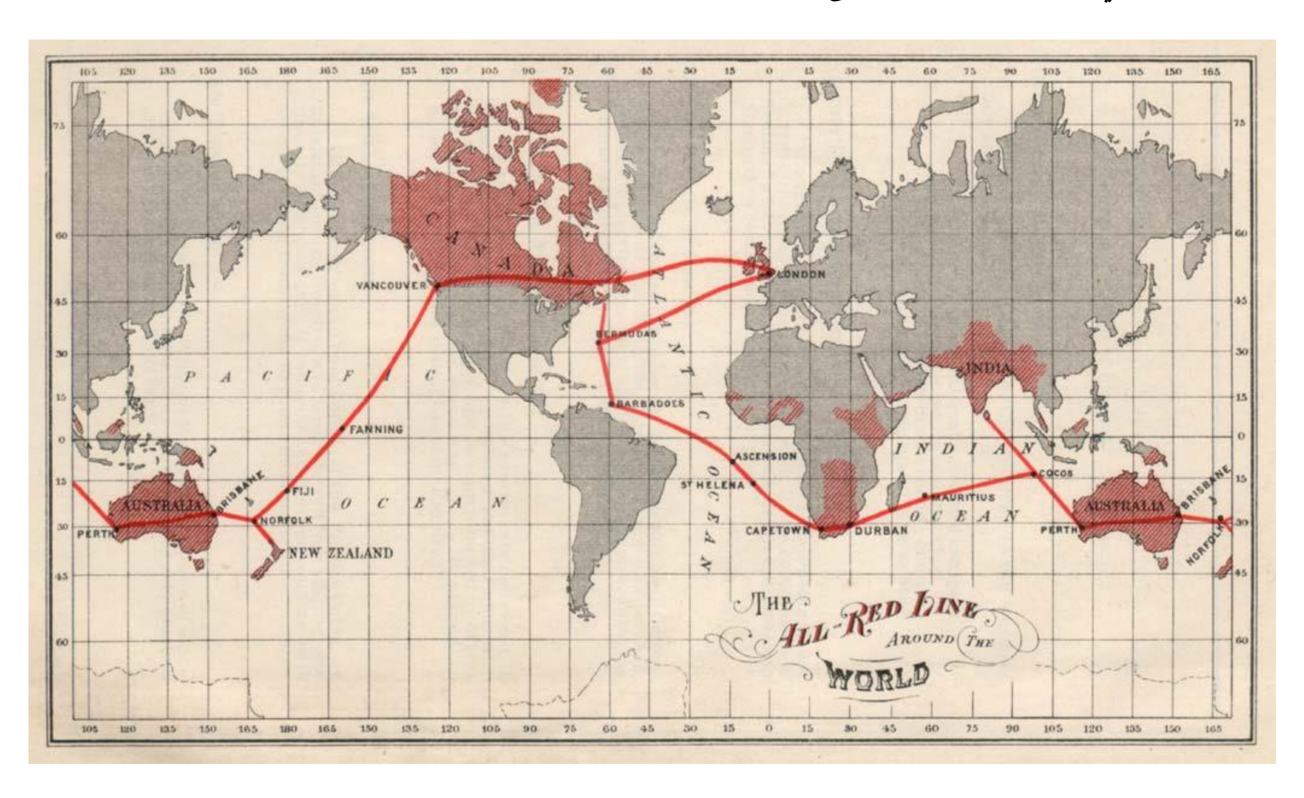
عندما ثبت أن هذه الجهود غير كافية، وجدت ألمانيا النجاح في الهيئات المتعددة الأطراف لوضع المعايير. ففي عام 1906، نجحت ألمانيا في تنظيم مؤتمر بخصوص معايير الاتصال اللاسلكي يضم القوى العظمى معًا، للتوصل إلى أول اتفاقية دولية للتلغراف اللاسلكي. في هذا المؤتمر، أجمع الأعضاء على حظر سياسة "عدم الاتصال المتبادل" لماركوني، فكسروا الاحتكار البريطاني وأرسوا الاحتكار الأنجلو ألماني الفعال.[23]

تكشف المنافسة الأنجلو ألمانية عن أن هيئات وضع المعايير تخلف عواقب إستراتيجية هائلة. وتستخدم الصين اليوم العديد من النُهج التي استخدمتها ألمانيا قبل قرن من الزمان — السياسة الصناعية التي تقودها الدولة، وحماية الدولة، والعقود الحكومية السخية، والتكامل المدني العسكري، وحظر المنتجات المنافسة، وعمليات الاندماج القسري، واستهداف الأسواق الناشئة، بل ومعاهدات دولية لوضع معاييرها — وكل هذا قد ساعد شركات التكنولوجيا الصينية مثل علي بابا وتينسنت، اللتين تمتلكان منصتَي WeChat وAliPay، على التحول إلى أبطال محليين. ومنذ ذلك الحين، وسّعت هذه الشركات نشاطها ليمتد إلى الخارج، وغالبًا لا تستهدف السوق الأمريكية فحسب، بل الأسواق الناشئة التي تتسم بانخفاض الأرباح وانخفاض القدرة التنافسية، تمامًا كما فعلت شركة تيليفونكن الألمانية من قبلها.[24]

تتنافس الصين أيضًا على المعايير في البنية الأساسية المادية لاتصال الإنترنت. وتستثمر حكومتها المليارات حتى تتمكن شركات تصنيع الشرائح في الصين من التغلب على المنافسين الأمريكيين في السباق على معايير الجيل الخامس لشبكة إنترنت الأجهزة المحمولة. وعلى نحو مماثل، تتلقى شركات صينية مثل هواوي وزد تي إي قروضًا حكومية لبناء البنية الأساسية المادية لاتصال الإنترنت في مختلف أنحاء العالم النامي. وكما يُظهِر المثال البريطاني، فإن هذه الجهود لا تجعل التكنولوجيا الصينية المعيار فحسب، بل تعطيها أيضًا الفرص للمراقبة والرصد. من ناحية أخرى، تزيد مبادرة الحزام والطريق من احتمال أن تضع الصين معايير "البنية الأساسية الذكية" في مختلف أنحاء آسيا، وخصوصًا أجهزة الاستشعار والبرامج ذات الصلة، وقد تحرم الشركات الأخرى من القدرة على التشغيل البيني، ومن ثَمَّ تحرمها من المركبات ذاتية القيادة وغيرها من الصناعات.

تُظهِر المنافسة الأنجلو ألمانية في مجال التلغراف أن واشنطن تحتاج إلى التعامل بجدية مع التحدي الذي تفرضه دولة الصين على المعايير. وهي تطرح أيضًا وسيلة للمضي قدمًا. وعلى النحو نفسه الذي استخدمت به ألمانيا المؤتمرات الدولية لكسر الاحتكار البريطاني للتلغراف، فإن الولايات المتحدة تستطيع أن تضع معايير مواتية لتكنولوجيا المعلومات والاتصالات أو تحافظ عليها من خلال اتفاقيات متعددة الأطراف. والقيام بهذا قد يُبعد الصين عن وضع المعايير من جانب واحد من خلال اتفاقيات التجارة الحرة، أو الشركات العملاقة في الدول، أو مشروعات البنية الأساسية.

3. بريطانيا في الحرب العالمية الأولى: نشر الهيمنة المعلوماتية



يمثل "الخط الأحمر بكامله" شبكة مكلفة من خطوط الكابلات الممتدة تحت سطح البحر التي أنشئت بما يزيد على الحاجة بكثير وقد تم تمديدها بحيث لا تمر في أي جزء عبر أراضٍ منافسة. وكان عدم كفاية استثمار ألمانيا في شبكة الاتصالات العالمية المرنة الخاصة بها سببًا في تمكين بريطانيا من قطع اتصالاتها العالمية في حين ظلت بريطانيا غير متأثرة عمومًا.

المصدر: / *George Johnson, ed.,* The All Red Line: The Annals and Aims of the Pacific Cable Project / Internet Archive[25]

لم تكن الجهود التي بذلتها ألمانيا لكسر الهيمنة البريطانية على الاتصالات في أوائل القرن العشرين نابعة من جنون العظمة. فبمجرد اندلاع الحرب العالمية الأولى، نجحت بريطانيا في فرض نفوذها الكبير على شبكات الاتصالات لتشكيل مسار الحرب. حيث قطعت الكابلات الألمانية، وراقبت عمليات الإرسال الألمانية، وأجبرت حركة الاتصالات الألمانية على الدخول في الشبكات التي تسيطر عليها بريطانيا ـ ما أدى إلى اكتشاف برقية زيمرمان وفك شفرتها، الأمر الذي ساعد على حمل أمريكا على الدخول في الحرب.[26]

لم تكن بريطانيا العظمى أول قوة عظمى تقطع شبكات الاتصالات أو تستغلها: فقد قطعت بيرو الاتصال بين تشيلي وبوليفيا، وقطعت الولايات المتحدة الكابلات الإسبانية، وقامت بريطانيا بعزل البوير عن مؤيديهم الأوروبيين في إحدى الأزمات، واستفادت من حركة الاتصالات الكابلية المتجهة إلى فرنسا في أزمة أخرى.[27] لكن وصلت هذه الجهود ذروتها في الحرب العالمية الأولى.

كانت بريطانيا العظمى أول من تعزل دولة كاملة عن شبكات الاتصالات العالمية الرئيسية، وتنشر في اليوم الأول من الحرب خطة تم وضعها بعناية في وقت السلم.[28] وفي غضون عام، دمرت بريطانيا العظمى الكابلات الألمانية في مختلف أنحاء العالم: في القنال الإنجليزي، وبحر الشمال، وشمال الأطلسي، وأمريكا الجنوبية، وجزء كبير من إفريقيا، والشرق الأقصى، بل وفي البلدان المحايدة التي كانت تستضيف البنية الأساسية الألمانية.[29]

وفي محاولة للتعويض، حاولت ألمانيا توسيع الشبكة اللاسلكية التي شيدتها شركة تيليفونكن قبل عشرة أعوام في أمريكا اللاتينية و"بلدان الجنوب" حتى تغطي العالم. في محاولة موازية حديثة لطريق الحرير الرقمي في الصين، قدمت برلين قروضًا واستثمارات إلى الحكومات المهتمة "بالفوائد الإنمائية في مجال الاتصال اللاسلكي" حتى تتسنى لها استضافة عُقد الاتصال الألمانية. وردًا على ذلك، أقنعت بريطانيا العظمى أغلب هذه البلدان أو حثتها على التخلي عن دعم عُقد الاتصال اللاسلكي الألمانية أو قامت بتخريب هذه العُقَد تمامًا.[30]

عندما لم تعد لبرلين شبكات خاصة بها، لم يكن أمامها خيار آخر سوى الاعتماد على شبكة بريطانيا في أثناء الحرب. في البداية، بدأ البريطانيون في صمتٍ بمراقبة حركة الاتصالات بالكامل التي مرت عبر كابلاتها، واستخدموا هذه الميزة لشن حرب معلوماتية ضد ألمانيا، فقاموا بتسريب بعض الاتصالات الألمانية المحرجة عن عمد للإضرار بعلاقاتها مع الدول المحايدة. فعندما أرسلت ألمانيا برقية تقترح فيها إنشاء تحالف عسكري مع المكسيك ضد الولايات المتحدة ـ برقية زيمرمان الفاضحة ـ اجتاحت هذه الرسالة شبكة بريطانية، ثم اعترضتها بريطانيا العظمى وقامت بفك شفرتها، ثم أخبرت بها حكومة الولايات المتحدة، التي بدورها كشفت عن هذه الرسالة للرأي العام الأمريكي.[31] ولقد ساعد ذلك الحادث على حمل الولايات المتحدة على الدخول في الحرب وتشكيل تاريخ العالم لتكون هزيمة ألمانيا هزيمة حتمية في نهاية المطاف.

إن حرب المعلومات البريطانية ضد ألمانيا تكشف عن المخاطر المترتبة على منح قوة منافسة القدرةَ على مراقبة حركة الاتصالات لدولة ما أو منعها من الوصول إلى الاتصالات السلكية واللاسلكية. كما تكشف عن أن الشبكات التي تراها القوى العظمى أمورًا مسلّمًا بها في وقت السلم غالبًا ما يتم الحرمان منها في زمن الحرب، وأن الصراع على عُقد الاتصالات سيمتد حتمًا ليشمل أطرافًا ثالثة ودولاً محايدة.

4. فوز ألماني في تاننبرغ: مخاطر الاعتراض



محطة ألمانية ميدانية للتلغراف اللاسلكي خلال الحرب العالمية الأولى. أدى عجز روسيا عن تشفير اتصالاتها بشكل كافٍ في محطاتها الميدانية إلى هزيمة كارثية أعادت تشكيل مسار الحرب.

المصدر: [32]*C. O. Nordensvan and Valdemar Langlet,* Det stora världskriget *[The Great World War]*

لم تكن ألمانيا تفتقر تمامًا إلى قدراتها الخاصة في مجال حرب المعلومات. فقد قطعت كابلاتٍ روسيةً برية وبحرية كانت تصل روسيا بحلفائها في الغرب، فضلاً عن العديد من الكابلات العابرة للمحيط الأطلسي التي اعتمد عليها البريطانيون، لتكون ألمانيا أول دولة تستخدم الغواصات لتنفيذ هذه المهام.[33] ونظرًا إلى التمديدات الزائدة في الشبكات البريطانية، فإن هذه الجهود كانت في نهاية المطاف أقل إضعافًا مما كان يتمناه الألمان. وكان الأمر الأكثر أهمية استخدام ألمانيا للاستخبارات الراديوية ضد روسيا في معركة تاننبرغ في أغسطس/آب 1914، أي الشهر الأول من الحرب، الأمر الذي عجل بهزيمة كارثية للروس. في ذلك الوقت، أطلق أحد ضباط الاستخبارات الألمان على الحادث وصف "الحادث الأول في تاريخ البشرية الذي أدى فيه اعتراض الاتصالات اللاسلكية المعادية دورًا حاسمًا".[34]

وقعت المعركة وسط مكاسب روسية على الجبهة الشرقية. وعند توغل روسيا في أعماق أبعد في روسيا الشرقية، واجه الجيش الروسي تحديًا كبيرًا في الاتصالات كان يعد تمهيديًا لهزيمة كارثية. فقد قطع الألمان المنسحبون خطوط التلغراف الخاصة بهم، وكان الروس المتقدمون يفتقرون إلى الطاقم المدرب بشكل كافٍ لإنشاء اتصالات سلكية عبر تشكيلهم غير المنظم. وكان الإرسال اللاسلكي حلاً بديلاً، لكن في الوقت الذي اعتمد فيه الروس تقنيات اتصال لاسلكي جديدة في عمليات القيادة والتحكم العسكرية، لم يتمكنوا من تأمينها بشكل كافٍ. فقد تم تخصيص أنظمة تشفير لمجموعات مختلفة؛ وكان أغلبها لم يتلق إلا القليل من التدريب على إشارات التشفير وفك التشفير؛ وكان من المعروف أن البريطانيّين تمكنوا من فك بعض الشفرات؛ وكانت كتب الشفرة محدودة أو غير مفهومة بالنسبة إلى كثير من المجندين الأميين.[35] فكانت النتيجة أن القادة الروس شعروا بأنهم مضطرون إلى المجازفة واستخدام رسائل لاسلكية غير مشفرة على أمل ألا يرصدها الألمان رصدًا دقيقًا.

لكن الألمان كانوا يراقبون هذه الإشارات عن كثب. وبعد أن لاحظوا عدم انضباط الاتصال اللاسلكي الروسي في الحرب ضد اليابانيين، أدركوا أن عمليات الإرسال الروسية غير المشفرة ليست جزءًا من محاولة خداع. ثم استخدموا معرفتهم بالاتصالات الروسية في الوقت الحقيقي لرفع "ضباب الحرب" وهزيمة القوة المتفوقة هزيمة حاسمة. فخسرت روسيا جيشًا كاملاً، حيث سقط أكثر من 100000 قتيل، وتم أَسرُ 92000 سجين مقابل 13000 قتيل ألماني فقط.

5. بريطانيا في الحرب العالمية الثانية: حدود التشفير



التروس الميكانيكية الدوارة لآلية التشفير لورينز التي وصفت بأنها غير قابلة للاختراق فعليًا خلال الحرب العالمية الثانية. إنَّ الجهود البريطانية لفك نظام التشفير هذا منحت المسؤولين القدرة على الوصول إلى الاتصالات الألمانية عالية المستوى.

المصدر: Matt Crypto / Wikimedia Commons[36]

جلبت اختراعات الإرسال التلغرافي اللاسلكي والراديو قدرًا أكبر من الراحة مقارنة بالكابلات المادية، لكنها انطوت على مخاطر اعتراض أكبر. في الحربين العالميتين الأولى والثانية، كانت القوى العظمى موجودة في عالم كان من المفترض أن تكون الاتصالات اللاسلكية فيه متاحة للآخرين. وفي عالم كهذا ـ لا تختلف افتراضاته كثيرًا عن الافتراضات الحالية بشأن مدى إمكانية تعرض أنظمة الكمبيوتر والاتصالات الحديثة للخطر ـ كان التشفير يشكل أهمية بالغة بالنسبة إلى الأمن. وكانت النتيجة على حد تعبير أحد المؤرخين العسكريين الأمريكيين هي "الصراع بين واضع الشفرة ومحلل الشفرة".[37] وعندما لا تكون القوى العظمى على الجبهة الصحيحة في ذلك الصراع، فإن النتائج قد تكون مأساوية.

لتجنب حدوث هذه النتيجة، فإن المنظمات تستخدم أنظمة التشفير للحد من خطر مساس هذا الاعتراض بالأمن. كما مارست "الانضباط اللاسلكي" لمنع الخصوم من استخلاص التفاصيل الدقيقة لأنماط الاستخدام من خلال تحليل الاتصالات اللاسلكية.

لقد استثمرت أغلب القوى العظمى في جهود صناعية حقيقية تهدف إلى دراسة اتصالات الخصم، بل وفي فك أنظمة تشفير الخصم إن أمكنها ذلك. وكانت بريطانيا العظمى أكثر مركزية في تحليلها لأنظمة تشفير الخصم مقارنة بألمانيا، التي نشرت هذه الوظائف بين العديد من الوكالات. وتمامًا كما كانت النجاحات التي حققتها بريطانيا في استخبارات الإشارات وتحليل التشفير سببًا في تشكيل مسار الحرب العالمية الأولى، فإنها أيضًا شكلت مسار الحرب العالمية الثانية عندما نجحت العملية البريطانية في مركز بليتشلي بارك في فك شفرات نظامَي التشفير الألمانيين إنيجما ولورينز.

فقد استخدم نظاما التشفير إنيجما ولورينز آلات ذات تروس دوارة معقدة جدًا لتشفير الرسائل التي تصورت ألمانيا أنها "ستظل محصنة ضد الاعتراض".[38] كل ضغطة مفتاح تستبدل حرفًا بآخر وفق إعدادات فريدة للآلة، وتلك الإعدادات ــ التي تجاوزت إجمالي عدد الذرات في الكون بالنسبة إلى نظام لورينز ــ كانت تحتاج إلى مشاركتها بين المرسل والمستقبل

لقراءة الرسالة.[39] وكانت آلة إنيجما تُستخدم من قِبَل المؤسسة العسكرية جيستابو والدبلوماسيين؛ أما آلة لورينز، التي كانت أكثر تعقيدًا، فكان يستخدمها أدولف هتلر وكبار المسؤولين النازيين والعسكريين للتواصل في ما بينهم.

كان النجاح البريطاني في فك شفرات إنيجما ولورينز نتاجًا لعدة تطورات. أولاً، كان ذلك نتاجًا للتعاون الاستخباراتي المتحالف مع بولندا، التي استغلت بعض الأخطاء الألمانية لفك شفرات بعض آلات إنيجما البسيطة.[40] وعلى حد تعبير أحد المحللين البريطانيين للشفرات في ذلك الوقت، فإن جهودهم "ما كانت لتحرز نتيجة أبدًا" من دون الإسهامات البولندية.[41]

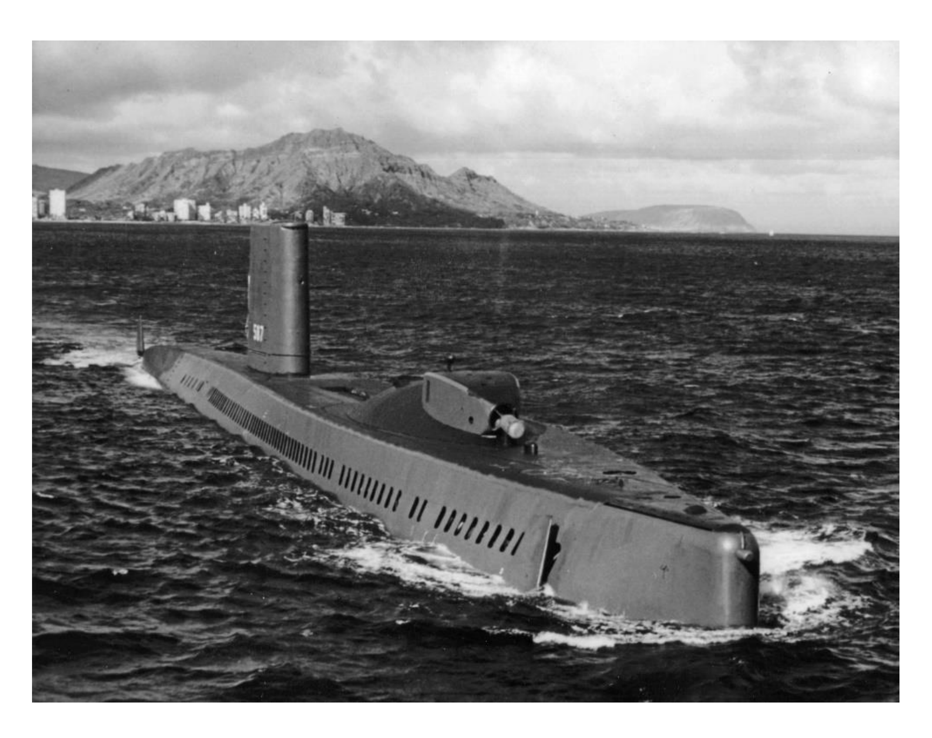
ثانيًا، كان ذلك نتاجًا لثقة ألمانيا المفرطة، حيث لم تكن ألمانيا تشك على الإطلاق في إمكانية فك تشفير أنظمتها ومن ثَمَّ لم تولِ اهتمامًا للتعديلات البسيطة التي كانت لتجبر بريطانيا على البدء في جديد.[42] وعلى الرغم من ذلك، فإن إيمان ألمانيا باستحالة فك تشفير آلياتها "كان على حق تقريبًا"، كما روى أحد كبار المسؤولين في مركز بليتشلي بارك.[43]

وأخيرًا، كان نتاجًا لهفوة واحدة وجسيمة في "الانضباط اللاسلكي" الألماني التي أتاحت الفرصة لإجراء هندسة عكسية لأنظمة التشفير الألمانية وكشفها على الرغم من أنه لم تسبق رؤية أحد هذه الأنظمة رؤيا عين على الإطلاق.[44] حتى أكثر الأنظمة تعقيدًا كانت عُرضة لخطأ المستخدم، وكان بوسع الخصم اليقظ أن يستغلها.

بفك شفرات "إنيجما" و"لورينز"، أصبح لبريطانيا العظمى وصول إلى بعض من أكثر الاتصالات حساسية في ألمانيا. وقد ورد أن ونستون تشرشل قد أشاد بالمخابرات بوصفها السبب الرئيسي لفوز بريطانيا العظمى في الحرب، كما ورد أن دوايت أيزنهاور وصفها بأنها "حاسمة".[45] ويزعم المؤرخ الرسمي للاستخبارات البريطانية، فرانسيس هاري هينسلي، أن هذه النجاحات "اختصرت فترة الحرب بما لا يقل عن عامين وربما أربعة أعوام"، حيث تم تقويض المارشال إرفين رومل في إفريقيا، وإلحاق خسائر فادحة بالغواصات الألمانية التي دمرت سفن الحلفاء، ونجاح عمليات الإنزال في نورماندي.[46] كما ساعدت هذه الاتصالات بريطانيا على كشف كل الجواسيس الألمان تقريبًا الذين يدخلون البلاد وتجنيدهم أو استخدامهم غالبًا لتوصيل معلومات استخباراتية خاطئة، حيث أشار مدير البرنامج إلى أن الاستخبارات البريطانية "أدارت نظام التجسس الألماني في هذا البلد وأحكمت سيطرتها عليه".[47] ولم تكن هناك إلا دول قليلة تمتلك معلومات دقيقة كهذه عن دولة أخرى في زمن الحرب.

وعند وضع كل العناصر في الحسبان، فإن النجاحات التي حققتها الجهود البريطانية في مواجهة ألمانيا، ومراقبة بولندا للاتصالات الألمانية في وقت السلم، والقرار الذي اتخذته بخصوص مشاركة المعلومات التي اخترقتها مع بريطانيا العظمى ستشكل دروسًا يستفاد منها اليوم عندما تقوم القوى العظمى بعمليات استطلاع سيبراني ضد بعضها. وعلى نطاق أوسع، فإن أولئك الذين يرون أن التشفير من شأنه أن يخفف من مشكلات قدرة الخصم على الوصول إلى شبكة الاتصالات لدولة منافسة ربما يرتكبون خطأ لا يختلف عن ذلك الذي ارتكبته ألمانيا نفسها ذات يوم: الثقة المفرطة في التكنولوجيا والانتباه المحدود إلى احتمال الخطأ البشري الوارد دائمًا.

6. عملية آيفي بيلز: أعماق البحث عن المعلومات



غواصة يو إس إس هلبوت التي ورد أنها شاركت في محاولة التنصت على خط هاتفي سوفييتي تحت سطح البحر.

المصدر: U.S. Navy / Wikimedia Commons[48]

كان الاتحاد السوفييتي أكثر حرصًا بخصوص التشفير مقارنة بالنازيين، حيث اعتمد على نسخته الخاصة من آلة إنيجما ـ المعروفة باسم فيالكا ـ التي كانت أكثر تعقيدًا إلى حد كبير.[49] لهذا السبب، فإن الكم الهائل من المعلومات الاستخباراتية على المستوى الإستراتيجي التي نتجت في الحرب العالمية الثانية بعد فك أنظمة التشفير الألمانية لم يكن له نظير معروف في الحرب الباردة. في ضوء هذه التحديات، اتُّبِعت أساليب أخرى لاختراق اتصالات الخصم. وكان أحد أكثر هذه الجهود جرأة مرتبطًا بالكابلات تحت سطح البحر.

أدى ظهور الكابلات البحرية في القرن التاسع عشر في نهاية المطاف إلى بذل جهود لقطع هذه الكابلات والتنصت عليها من حين إلى آخر، وغالبًا ما كان يحدث ذلك في المياه الضحلة أو في الأراضي التي كانت هذه المهام فيها أسهل. على النقيض من ذلك، كان من المعتقد أن تنفيذ هذه العمليات في المياه العميقة التي تقع تحت سيادة الخصم كان مستحيلاً في واقع الأمر، خصوصًا إذا كان من الضروري تنفيذها سرًا. وبداية من القرن العشرين، توصلت بريطانيا والقوى العظمى التي لحقتها إلى رأي حاسم بخصوص أمن الكابلات البحرية: إذا كانت مواقع الإنزال مؤمنة، ولم تعبر الكابلات البلدان المحايدة أو غير الصديقة، فإنها بشكل عام تكون مؤمنة ضد الاعتراض وضد القطع غالبًا، خصوصًا في وقت السلم.[50]

لكن في أثناء الحرب الباردة، تغيرت هذه الحسابات. حيث فتح ظهور الغواصات النووية الباب أمام إمكانية التنصت على الكابلات الممتدة تحت سطح البحر في مياه أعمق. لكن كان من المعتقد أن مهمة إرسال الغواصين للوصول إلى الكابلات في قاع البحر أقرب إلى استكشاف الفضاء من المحاولات المعتادة للاستفادة من الكابلات التي جرت في عصور سابقة. وكان إنشاء توصيلة تنصت يمكن تركيبها في مثل هذه الظروف أمرًا بالغ الصعوبة من الناحية الفنية أيضًا.

وعندما اشتبهت الولايات المتحدة في أن كابلاً سوفييتيًا تحت سطح البحر قد يكون ممتدًا من المقر البحري في فلاديفوستوك إلى قاعدة غواصات في شبه جزيرة كامشاتكا، سعت إلى التغلب على العقبات التي يمكن أن تواجهها، ما يظهر قيمة استخبارات الإشارات.[51] وكان من المعتقد أن التنصت على حزمة الأسلاك التي يبلغ قطرها خمس بوصات من شأنه أن يوفر معلومات بالغة الأهمية عن القوات النووية السوفييتية.[52] وعلى الرغم من أن السوفييت قاموا بتشفير كل حركة الاتصالات المرسلة عبر

الهواء، فإن الولايات المتحدة توقعت أن السوفييت سيفترضون أنه من المستحيل تقريبًا الوصول إلى الكابل المحمي تحت سطح البحر، ومن ثَم فلن يقوموا بتشفيره. إضافة إلى ذلك، فإن "الأدميرالات والجنرالات السوفييت سيكونون أكثر تعجرفًا وأقل صبرًا على تحمل تخصيص كم هائل من واضعي الشفرة لذلك حيث إنهم منهمكون بالفعل في الجزء الأكبر من عملهم"، وسوف يصرون على الاتصالات الصوتية غير المؤمنة.[53] ومن ثم فإن توصيلة التنصت ستوفر معلومات استخباراتية قيمة ونادرة، فأطلقت البحرية الأمريكية عملية آيفي بيلز لإنشاء هذه التوصيلة.

لا يزال الكثير عن عملية التنصت والمعلومات الاستخباراتية التي تم الحصول عليها سريًا، لكن المصادر العلنية توضح بعض التفاصيل عن العملية الفريدة والمبتكرة. أرسلت الولايات المتحدة غواصة نووية، وهي غواصة يو إس إس هلبوت، للتسلل بهدوء عبر البحرية السوفييتية والعثور على الكابل البحري في منطقة تمتد إلى 600000 ميل مربع.[54] وتم ابتكار تقنية حديثة لضمان عمل الغواصين تحت ضغوط شديدة وفي مياه شديدة البرودة لعدة ساعات. وعلى نحو مماثل، تم ابتكار أساليب جديدة لإنشاء توصيلة تنصت في هذه البيئة العصيبة.[55] كان من الضروري أن يتم كل هذا من دون أي اكتشاف أو شكوك من قِبل السوفييت. لأنه إذا اكتشف السوفييت هذه الغواصة، فسرعان ما سيكونون على متنها أو سيقومون بتدميرها.

نجحت العملية في نهاية المطاف، وطوال سبعينيات القرن العشرين، كانت البحرية الأمريكية تتنصت على الرسائل غير المؤمنة المارة عبر الكابل وتقوم بتسجيلها. وكل بضعة أشهر، كانت الغواصات الأمريكية تتسلل بهدوء إلى المياه السوفييتية، متفادية الغواصات الهجومية، وتنشر الغواصين على خطوط الكابل المتنصت عليه، وتستعيد أشرطة الاتصالات السوفييتية ـ ما أفادهم في الحصول على معلومات استخباراتية نادرة وقيمة للغاية. وعلى الرغم من أن الولايات المتحدة قامت بتوسيع "شبكة التجسس لتضم أقمارًا، وطائرات، ومحطات للتنصت، وغواصات" لجمع استخبارات الإشارات، فإنها "لم تتمكن من اختراق خط هاتفي سلكي" داخل أراضي أحد الخصوم. وقد أوضح هذا الجهد التحول التطوري في الاتصالات، أي أن البيانات والإشارات المرسلة عبر أي وسيط وبأي وسيلة يمكن الوصول إليها من جانب دولة مصمِّمة تتسلح بالأدوات المناسبة. وعلى الرغم من أنه في النهاية تم اكتشاف توصيلة التنصت هذه بسبب بعض التسريبات عنها، فإن عمليات اعتراض الاتصالات التي تم تحقيقها قد وفرت معلومات استخباراتية عسكرية وسياسية لا تقدر بثمن للولايات المتحدة وحلفائها.[56]

المنافسة الحديثة في مجال الاتصالات السلكية واللاسلكية من منظور تاريخي

بحلول نهاية الحرب الباردة، كانت الولايات المتحدة قد حلت بوضوح محل بريطانيا العظمى بوصفها قوة مهيمنة على المعلومات. واحتفظت الولايات المتحدة بمكانة عقدية في شبكة الإنترنت العالمية، والقدرات الفضائية القوية، والهيمنة على معظم تكنولوجيا الإنترنت؛ وحسب ما تكشف التقارير المعلنة، فإنها تتمتع بإمكانات متطورة لاعتراض اتصالات الخصم أو حرمانه منها.

يجري الآن اختبار هذه المزايا الأمريكية، كما حدث مع بريطانيا العظمى قبل أكثر من قرن من الزمان. وهناك دول الآن مثل روسيا، والصين على وجه الخصوص، تتحدى الهيمنة الأمريكية. ففي حين تتمتع الولايات المتحدة بمكانة عقدية في العديد من تدفقات البيانات، فإن قوى أخرى تسعى بشكل متزايد إلى الحد من اعتمادها على الشبكات الأمريكية. وفي الوقت نفسه، فإن استخدام أمريكا مكانتها العقدية للاعتراض يعدّ أقل ضرورة مما كانت عليه بريطانيا العظمى قبل قرن من الزمان. فالإنترنت يجعل التدخل ممكنًا من الحاجة إلى السيطرة على البنية الأساسية المادية. ومن الممكن اختراق الهواتف الذكية وشبكات الكمبيوتر، وسواء تعرضت الاتصالات الحساسة للكشف بسبب وسائط التنصت المادية لعصر سابق أو بسبب التدخل الافتراضي لوسائط التنصت الحديثة، فإن النتيجة النهائية واحدة. ومن المرجح أن يؤدي الاتصال بهذه الطريقة إلى خلق ثغرة أمنية أكبر الآن مما كان عليه الحال في عصر التلغراف أو الراديو اللاسلكي.

كانت روسيا دولة رائدة في استغلال الثغرات الأمنية هذه. ففي عام 2007، شنت روسيا موجة من الهجمات الإلكترونية ضد مؤسسات إستونيا، التي كان أغلبها هجمات للحرمان من الخدمة.[57] وفي عام 2008، شنت هجمات إلكترونية في الحرب الروسية الجورجية. لم يقتصر الأمر على توجيه هجمات الحرمان من الخدمة فحسب، بل شمل أيضًا جهودًا لإعادة توجيه المواقع الإلكترونية الحكومية، والسيطرة على خوادم الحكومة الجورجية، وإعادة توجيه حركة بيانات الإنترنت في جورجيا من خلال خوادم خاضعة لسيطرة روسيا ـ حيث تم شن بعض الهجمات قبل اندلاع الصراع لتتزامن مع العمل العسكري الروسي.[58] وفي عام 2014، عندما غزت روسيا شبه جزيرة القرم، جمعت بين الهجمات الإلكترونية والسيطرة المادية على شبكات الاتصالات. استولى الجنود الروس على مرافق الاتصالات الأوكرانية، واستخدموها لقطع الاتصالات في شبه جزيرة القرم بل ولتنفيذ هجمات إلكترونية وتعطيل الاتصالات في أجزاء أخرى من أوكرانيا.[59] وفي عام 2015، بدأت روسيا موجة من الهجمات الإلكترونية على البنية الأساسية في أوكرانيا، فتسببت في انقطاع الطاقة عن مئات الآلاف من الأوكرانيين في حالتين رئيسيتين. وعلى مدى السنوات العديدة التي تلت ذلك، واصلت شن موجة من الهجمات غير المسبوقة في مختلف أنحاء أوكرانيا، التي امتدت لتشمل "وسائل الإعلام، والقطاع المالي، وقطاع النقل، والمؤسسات العسكرية والسياسية وقطاع الطاقة" ـ أي كل قطاعات المجتمع الأوكراني تقريبًا ـ في ما تصوره بعضهم أنه كان بمنزلة محاولة جزئية للتدريب على حملة مماثلة ضد الولايات المتحدة.[60] في الوقت نفسه، واصلت سلسلة من الهجمات عبر دول البلطيق وسعت كما هو معروف إلى تشكيل الانتخابات الأمريكية في عامَي 2016 و2020 من خلال حملات التضليل الإعلامي، فضلاً عن دول أخرى.[61] في عام 2021، اتهمت الحكومة الأمريكية روسيا رسميًا باختراق شركة تكنولوجيا المعلومات "سولارويندز"، وهو هجوم متطور أدى إلى كشف كثير من عمليات الحكومة الفيدرالية والعديد من الشركات الأمريكية الكبرى.[62]

تعد الصين هي القوة العظمى الأخرى التي تجري استثمارات ضخمة في المنافسة في مجال الاتصالات، وإن كانت على النقيض من روسيا، فإن الجهود التي تبذلها الصين لا تسعى إلى استغلال البنية الأساسية القائمة لشبكة الإنترنت فحسب، بل تسعى أيضًا إلى بناء شبكات وبنية أساسية يمكن أن تؤثر فيها بل وتسيطر عليها. ومثلها كمثل روسيا، كانت الصين بارعة في استغلال الثغرات الأمنية على الإنترنت. ففي أوائل العقد الأول من القرن الحادي والعشرين، شنت موجة من الهجمات على شبكات وزارة الدفاع الأمريكية أسمتها الوزارة "عملية تيتان رين".[63] وقد قدمت حكومات حول العالم ــ الولايات المتحدة، والمملكة المتحدة، وفرنسا، وألمانيا، وكندا، وأستراليا، واليابان، وكوريا الجنوبية، وتايوان، والهند، وأكثر من عشر حكومات أخرى ــ شكاوى من تدخل الصين في شبكاتها الحكومية. وقد أكد وزير العدل الأمريكي ويليام بار أن بعض أكبر الهجمات الإلكترونية خلال العقد الماضي قد ارتكبها عملاء صينيون، بما في ذلك عمليات سرقة سجلات من مكتب إدارة شؤون الموظفين الأمريكي (سجلات لعدد 21 مليون شخص)، ومجموعة فنادق ماريوت (لعدد 400 مليون نزيل)، وشركة أنثم للتأمين الصحي (لعدد 80 مليون شخص)، وشركة إيكويفاكس (لعدد 147 مليون شخص)، من بين مؤسسات أخرى.[64]

في الوقت نفسه، تضع الصين أيضًا حجر الأساس للبنية الأساسية للإنترنت في المستقبل، وفي ضوء جهودها السابقة، فمن غير المرجح أن يكون هذا الجهد لأغراض تجارية الآن أو أن يظل لأغراض تجارية محضة في الفترة المقبلة. والواقع أن استثمارات الصين تتجلى بأكبر قدر من الوضوح في شبكات الجيل الخامس التي من المتوقع أن تشكل حجر الأساس لاقتصاد أكثر ذكاءً واتصالاً يربط بين عدد لا يحصى من أجهزة الاستشعار وغيرها. ومن منطلق حرص الصين على بناء هذه الشبكات في مختلف أنحاء العالم، فقد عمِلت على دعم شركاتها العملاقة ومشروعاتها الرائدة في مجال تقنية الجيل الخامس في مختلف أنحاء العالم كجزء من مبادرة "طريق الحرير الرقمي". وبسبب الأسعار التنافسية، تمكنت شركات مثل هواوي من التفوق على غيرها من الشركات الكبرى في مجال بيع شبكات الجيل الخامس والاستحواذ على حصة كبيرة في السوق العالمية، الأمر الذي جعل الصين رائدة في بناء هذه الشبكات. وبعيدًا عن شبكات الجيل الخامس، قامت الحكومة الصينية بدعم الجهود الرامية إلى بناء البنية الأساسية للإنترنت أو الاتصالات في كل قارة تقريبًا. وتُكمَّل هذه الجهود كلها بحملة لصياغة المعايير العالمية، وهي أولوية سياسية رئيسية للصين منصوص عليها في وثائق التخطيط رفيعة المستوى، التي قد تُسهم ـ كما حدث في المنافسة الأنجلو ألمانية على الإرسال اللاسلكي قبل قرن من الزمان ـ في تشكيل مستقبل الاتصالات على نحو يفيد الصين. ولتحقيق هذه الغاية، كشفت الصين مؤخرًا عن مبادرة جديدة لأمن البيانات.[65]

يخشى البعض أن تترك أنشطة الصين الباب مفتوحًا أمام احتمال سيطرة بكين على هذه الشبكات بحكم الأمر الواقع، سواء لاعتراض حركة الاتصالات أو الحرمان من الوصول إليها. ولا يتوافر سوى قدر ضئيل من المعلومات المعلنة عن الجهود التي تبذلها الصين لتحقيق هذه السيطرة، لكن الحكومة الأمريكية كشفت في فبراير/شباط 2020 أن شركة هواوي وضعت أبوابًا خلفية في معدات شبكتها، ولم تكشف عنها للشركات ذات الصلة التي تعاقدت معها، وأن هذه الأبواب الخلفية تجاوزت تلك الأبواب التي تطلبها الحكومات المضيفة أحيانًا كجزء من عمليات الاعتراض القانونية.[66] فضلاً عن ذلك، كشفت التقارير العامة المعلنة أن شركة هواوي ساعدت حكومات مثل أوغندا وزامبيا على الكشف عن هويات المنشقّين عن هذه الحكومات.[67] بل عند النظر إلى ما هو أبعد من حالة هواوي، نجد أن شركة أمن إلكتروني قد اكتشفت مؤخرًا وجود أبواب خلفية في برنامج ضريبي إلزامي تطالب الحكومة الصينية الشركات الأجنبية بتثبيته.[68] وبصرف النظر عما إذا كانت هذه الحالات تشير إلى أن هواوي نفسها قد استغلت مكانتها في هذه الشبكات، فإن سلوك الشركة وسجل الصين الحافل بالهجمات الإلكترونية وعمليات التجسس، هما من الأسباب التي تدعو إلى القلق.

السبب الرئيسي الآخر وراء القلق ينبع من التاريخ بل ومن سلوك القوى العظمى الليبرالية الأكثر تقيدًا بحكم القانون. والواقع أن الحالات التاريخية السابقة تشير بشكل بارز إلى أن ذلك النوع من القوة والنفوذ الذي قد تمارسه شركة مثل هواوي من المرجح أن تستغله الحكومة الصينية، تمامًا كما كانت القوى العظمى الأخرى كثيرًا ما تستغل مكانة شركاتها أو قدراتها في مجال الاتصالات.

من هذا المنظور التاريخي الأوسع، قد تدفع الأدلة العديد من المراقبين إلى استنتاج أن الحيطة والحذر مُبرَّران في ما يتعلق بدور هواوي في شبكات الاتصالات ـــ حتى وإن كانت دوافع الشركة هي بالفعل تجارية بحتة، وكانت وعودها "بعدم وجود الأبواب الخلفية والتجسس" جديرة بالثقة، وكانت بكين صادقة في التزامها بالوفاء بهذه التعهدات.

على نطاق أوسع، وكما يبين هذا التقرير، فإن العديد من سمات المنافسة بين القوى العظمى في مجال الاتصالات التي تعد جديدة اليوم لها جذور في الماضي. وعلى مر التاريخ، تكررت سيناريوهات عديدة:

- *القوة:* كانت السيطرة على شبكات الاتصالات السلكية واللاسلكية شكلاً من أشكال القوة السياسية منذ إنشائها قبل أكثر من 150 عامًا. فقد استغلت بريطانيا العظمى دورها في الاتصالات والإرسال اللاسلكي، ومن المرجح أن الولايات المتحدة قد فعلت ذلك في عصر الإنترنت الحديث، وهناك من الأسباب ما يدعونا إلى القلق من أن تحاول الصين القيام بذلك اليوم.

- *اللامبالاة:* قد أدت فترات طويلة من السلام والازدهار إلى حالة من اللامبالاة إزاء مخاطر الاتصالات. ففي القرن التاسع عشر، كانت القوى العظمى قانعة بالاعتماد على الشركات الأجنبية والشبكات التي تديرها جهات أجنبية، تمامًا كما هو الحال مع الدول اليوم التي أظهرت استعدادها لقبول معدات الاتصالات الصينية وتشغيلها. لكن في نهاية المطاف، أثبت الاعتماد على المنافسين أو الخصوم المحتملين أنه كارثة بالنسبة إلى دول مثل ألمانيا وأعاد تشكيل السياسة العالمية.

- *الاستغلال:* قد أدت تكنولوجيا الاتصالات الجديدة دومًا إلى بذل جهود جديدة لاعتراضها، أو الحرمان منها أو استغلالها. وعلى الرغم من الآمال في أن يؤدي التشفير إلى تعقيد الجهود التي تبذلها الصين لاعتراض الاتصالات الحديثة، فإن الفترات السابقة وضعت أملاً كبيرًا في التشفير وقد تحطم هذا الأمل بسبب خطأ المستخدم والجهود الحثيثة التي بذلتها الدول المنافسة لاختراق هذه الاتصالات، كما هو الحال عندما اكتشفت ألمانيا أن بريطانيا العظمى استطاعت أن تفك شفرة أنظمتها التي وصفت بأنها "غير قابلة للاختراق". فلا بد أن يكون التواضع مصاحبًا لكل موجة من التقنيات التي يفترض أنها مؤمنة.

- *الشركات العملاقة:* تسعى الدول في كثير من الأحيان إلى الفوز بشركاتها العملاقة في الاتصالات، خصوصًا مع تصاعد التوترات بين القوى العظمى. وتفخر حكومة الصين بإنجازات شركة هواوي، وتؤيدها في مختلف أنحاء العالم - بل إنها تهدد الدول التي ترفض تكنولوجيا هذه الشركة. ومن غير المعتاد أن تكون أي شركة قريبة للغاية من حكومتها محصنة ضد ضغوط الدولة، تمامًا كما حدث مع العديد من الشركات الأخرى العملاقة في مجال الاتصالات عبر التاريخ.

- *المعايير*: من الممكن أن تحدد معايير الاتصالات من الذي سيكون صاحب النفوذ على الشبكة، مثلما لجأت ألمانيا إلى هيئة وضع المعايير لكسر هيمنة بريطانيا العظمى على الإرسال اللاسلكي. واليوم، تجري هذه المنافسة في هيئات مثل الاتحاد الدولي للاتصالات، ويشير الدور الذي تؤديه شركة هواوي في هذه الهيئة إلى الحاجة إلى النظر هل معاييرها ستسمح للصين بإعادة تشكيل الاتصالات.

- *الحرمان:* لا يقتصر أمان الشبكة على الاعتراض وأمان البيانات، بل يتعلق أيضًا بمنع تشغيل الشبكة بالكامل أو الحرمان من الوصول إلى الشبكات الخارجية. فقد عزلت بريطانيا العظمى دولة ألمانيا عن شبكات التلغراف على مستوى العالم، وقد يعمل الدور الذي تؤديه شركة هواوي في الشبكات على تمكينها من إغلاق الشبكات في البلدان التي لها معدات تعمل فيها حتى لو كانت غير قادرة على الوصول إلى البيانات بسهولة.

- *التصميم:* تستهين دول كثيرة بالدرجة التي قد يبذل بها الخصم جهودًا غير عادية لاختراق شبكاتها، ثم تتعرض في ما بعدُ لمفاجأة غير سارة عندما يفعل الخصم ذلك. إن قدرة بريطانيا على فك الشفرات الألمانية في الحرب العالمية الثانية من خلال الجهود الصناعية والقدرةَ الأمريكية على التنصت على الكابلات البحرية الداخلية للسوفييت التي كان من المتصور أنه يستحيل التنصت عليها توضحان أعماق الجهود التي ستبذلها القوى العظمى للوصول إلى استخبارات الإشارات المهمة. ومن المرجح أن تبذل الصين أيضًا هذه الجهود القصوى، بل وإن وجدت شركة هواوي صعوبة في تسليح مكانتها في الشبكات الحديثة، فإن الاستهانة بحيلة المنافس المصمِّم ودافعه مثل الصين يشكل فكرة راسخة متكررة في المنافسة على الاتصالات.

كما يبين هذا التقرير، فإن العديد من سمات منافسة القوى العظمى على الاتصالات تظل على حالها، حتى مع اختلاف المتنافسين.

نبذة عن المؤلفين

راش دوشي: كان يشغل منصب مدير مبادرة إستراتيجية الصين في معهد بروكينجز وزميل برنامج السياسة الخارجية في معهد بروكنجز. كما كان زميلاً في مركز بول تساي الصيني التابع لكلية الحقوق بجامعة ييل، وكان عضوًا في الجلسة الافتتاحية لزمالة ويلسون تشاينا. ركزت أبحاثه على الإستراتيجية الصينية الكبرى فضلاً عن القضايا الأمنية في بلدان منطقة المحيطَين الهندي والهادئ. دوشي هو مؤلف كتاب *The Long Game: China's Grand Strategy to Displace American Order* أو *(اللعبة الطويلة: إستراتيجية الصين الكبرى لإزاحة النظام الأمريكي)*، المقرر صدوره قريبًا عن دار نشر جامعة أكسفورد. وهو يعمل حاليًا في إدارة بايدن.

كيفن ماكغينيس: عمل مؤخرًا في معهد بروكينجز كمعاود خارجي من برنامج Skillbridge التابع لوزارة الدفاع، حيث أسهم في مشروعات مختلفة داخل مركز دراسات السياسية لشرق آسيا. وهو من المحاربين القدامى في القوات الجوية، وأنهى مؤخرًا مدة خدمته كأستاذ في أكاديمية القوات الجوية الأمريكية، حيث كان يدرّس دورات في العلاقات الدولية والسياسة الآسيوية. كما عمِل مؤخرًا مساعدًا لشؤون البحوث لدى مركز دراسات الشؤون العسكرية الصينية التابع لمعهد الدراسات الإستراتيجية الوطنية، حيث ركز على برنامج تحديث جيش التحرير الشعبي وأمنه في منطقة المحيطَين الهندي والهادئ.

شكر وتقدير

يرغب المؤلفان في توجيه الشكر إلى المتدربين الداخليين السابقين إيزابيلا لو، وزيجين تشو، وجاوتشي تشانغ على مساعدتهم البحثية في هذا المشروع، والعديد من المراجعين الذين لم تذكر أسماؤهم، وكلير هاريسون وتيد راينرت على تحرير التقرير، وكريس كروبينسكي وراشيل سلاتري على التخطيط والتصميم على الويب. كما يعبّر معهد بروكينجز عن امتنانه لوزارة الخارجية الأمريكية ومعهد صحافة الحرب والسلام لتمويل هذا البحث.

---

[1] Steven Chase, Robert Fife, and Barrie McKenna, "Trudeau Refuses to Let 'politics Slip into' Decision on Huawei," *The Globe and Mail*, October 15, 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn and Josh Wingrove, "Trudeau Says Politics Won't Factor Into Huawei 5G Decision," *Time,* December 19, 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, *The Invisible Weapon*: Telecommunications and International Politics, 1851-1945 (Oxford, U.K.: Oxford University Press, 1991)، الفصل 1.

[3] المرجع ذاته، ترجع هذه الملاحظة إلى Headrick.

[4] المرجع ذاته

[5] المرجع ذاته

[6] المرجع ذاته، ترجع هذه الملاحظة إلى Headrick.

[7] Heidi Tworek, *News from Germany: The Competition to Control World Communications, 1900-1945* (New York: Harvard Historical Studies, 2019)..

[8] Daniel R. Headrick, *The Invisible Weapon*.

9 “NH 79949 Cienfuegos Cable-Cutting Operation, 11 May 1898,” Naval Historical Center Online Library, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.

10 Ibid., chapter 5. المرجع ذاته، الفصل 5.

11 Jonathan Winkler, “Information Warfare in World War I,” *The Journal of Military History* 73, no. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.

12 Cameron McR. Winslow, “Cable-Cutting at Cienfuegos," *The Century Illustrated Monthly Magazine* 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.

13 Jonathan Winkler, “Silencing the Enemy: Cable-Cutting in the Spanish–American War,” War on the Rocks, November 6, 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, “Manifesting Its Destiny: The U.S. Army Signal Corps in the Spanish-American War,” *Army History* 46 (1998): 14–21, https://www.jstor.org/stable/26304991.

14 Jonathan Winkler, “Silencing the Enemy.”

15 “Spanish American War: Telegraphy and Cable Cutting, Introductory Essay,” Naval History and Heritage Command, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.

16 Jonathan Winkler, “Silencing the Enemy.”

17 Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.

18 على الرغم مما ذكرته هايدي توريك، فإنه غالبًا ما كانت هناك مبالغة في ما يتعلق بدوره في تطوير هذه التقنية. Heidi Tworek, *News from Germany*.

19 Marc Raboy, “The First Company That Wanted to ‘Connect the World’ Wasn’t Google or Facebook,” Media@LSE, August 24, 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.

20 Heidi Tworek, *News from Germany*, 12–13.

21 Michael Friedewald, “Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914,” SSRN (January 9, 2014): https://doi.org/10.2139/ssrn.2375755.

22 المرجع ذاته

23 Marc Raboy, *Marconi: The Man Who Networked the World* (Oxford, U.K.: Oxford University Press, 2016), 226–28.

24 على سبيل المثال، كان عمل شركة تيليفونكن نشطًا حتى في المناطق التي لم يكن لألمانيا فيها وجود استعماري كبير، مثل أمريكا اللاتينية.

25 George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903), 10, at Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.

26 Gordon Corera, “How Britain Pioneered Cable-Cutting in World War One,” BBC News, December 15, 2017, https://www.bbc.com/news/world-europe-42367551.

27 Jonathan Winkler, “Information Warfare in World War I,” 847.

28 P. M. Kennedy, “Imperial Cable Communications and Strategy, 1870-1914,” *The English Historical Review* 86, no. 341 (1971): 728–52, https://www.jstor.org/stable/563928.

29 Jonathan Winkler, “Information Warfare in World War I,” 849.

30 Ibid., 851. المرجع ذاته، 851.

31 Gordon Corera, “Why Was the Zimmermann Telegram so Important?,” BBC News, January 17, 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, *Room 40: British Naval Intelligence 1914-18* (San Diego: Harcourt Brace Jovanovich, 1982).

32 C. O. Nordensvan and Valdemar Langlet, *Det stora världskriget* [The Great World War] (1915), at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.

33 Jonathan Winkler, “Information Warfare in World War I.”

34 Wilhelm Flicke, “The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer,” *NSA Cryptologic Spectrum Articles* 8, no. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.

35 Bruce Norman, *Secret Warfare: The Battle of Codes and Ciphers* (Newton Abbot, U.K.: David & Charles Ltd, 1973); Prit Buttar, *Collision of Empires: The War on the Eastern Front in 1914* (Oxford, U.K.: Osprey Publishing, 2014).

36 Matt Crypto, “The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum,” at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.

37 George I. Beck, “Military Communication - The Advent of Electrical Signaling,” Britannica, https://www.britannica.com/technology/military-communication.

38 Harry Hinsley, “The Influence of ULTRA in the Second World War” (lecture, Cambridge, U.K., October 19, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.

39 تقدَّر الإعدادات الممكنة بالصيغة 1×10^{170}.

40 “Bletchley Park Remembers Polish Code Breakers,” BBC News, July 14, 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.

41 Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (Cleobury Mortimer, U.K.: Classic Crypto Books, 1997).

42 Harry Hinsley, “The Influence of ULTRA.”

43 Ibid. المرجع ذاته

44 ارجع على سبيل المثال إلى Jerry Roberts, Lorenz: Jerry Roberts, *Lorenz: Breaking Hitler’s Top Secret Code at Bletchley Park* (Cheltenham, U.K.: History Press, 2017).

45 F. W. Winterbotham, *The Ultra Secret* (New York: Harper & Row, 1974), 154, 191.

46 Harry Hinsley, “The Influence of ULTRA.”

47 Calder Walton, “The Spies Who Came In From the Continent,” *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.

48 U.S. Navy, at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.

49 Anna Borshchevskaya, “The Soviets’ Unbreakable Code,” *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.

50 Daniel R. Headrick, *The Invisible Weapon*, chapter 4.

51 Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, *Blind Man’s Bluff: The Untold Story of American Submarine Espionage* (New York: Public Affairs, 1998), 222.

52 المرجع ذاته

53 Ibid., 223. المرجع ذاته، 223.

54 المرجع ذاته

55 Matt Blitz, “Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea,” *Popular Mechanics*, March 30, 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.

56 Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present* (Washington, DC: Georgetown University Press, 2013), 109–14; Matt Blitz, “Navy Divers.”

57 Damien McGuinness, “How a Cyber Attack Transformed Estonia,” BBC News, April 27, 2017, https://www.bbc.com/news/39655415; Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective,” (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

58 David Hollis, “Cyberwar Case Study: Georgia 2008,” Small Wars Journal, January 6, 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war,” *Security Dialogue* 43, no. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.

59 Pavel Polityuk and Jim Finkle, “Ukraine Says Communications Hit, MPs Phones Blocked,” Reuters, March 4, 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, “Russian Electronic Warfare in Ukraine: Between Real and Imaginable,” Jamestown Foundation, May 24, 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.

[60] Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” U.S. Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, “The impact of Russian interference on Germany’s 2017 elections,” (congressional testimony, June 28, 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller, “US intel agencies blame Russia for massive SolarWinds hack,” *The Hill,* January 5, 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] “Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain,” Council on Foreign Relations, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, “China’s Hacking Spree Will Have a Decades-Long Fallout,” *Wired*, February 11, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong, “China Launches Initiative to Set Global Data-Security Roles,” *The Wall Street Journal,* September 8, 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, “U.S. Officials Say Huawei Can Covertly Access Telecom Networks,” *The Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo, and Josh Chin, “Huawei Technicians Helped African Governments Spy on Political Opponents,” *The Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, “Hidden Back Door Embedded in Chinese Tax Software, Firm Says,” Bloomberg, June 25, 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.